AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Claims 1-4 – cancelled.

5. (New) A method of enforcing a network policy on a user connected by way of a respective edge switch to a packet – based communication network which has a network core and a plurality of edge switches, the method comprising:

(a) enabling control message snooping for each of said edge switches;

(b) obtaining the network address of said user;

(c) forwarding to said user from a policy server a unicast request packet which has the network address of said user as a destination address, includes a control message protocol header that identifies said unicast packet as a request packet and includes a payload.

(d) in response to reception of said request packet at said user, returning a reply packet which identifies said reply packet as a reply packet with an unmodified payload;

(e) at said respective edge switch, responding to said reply packet to divert said reply packet to a management agent for said respective edge switch;

(f) modifying said payload;

(b) returning to the server said reply packet including said payload as modified, said reply packet as returned to said server containing an identification of said respective edge switch and said user; and

(h) providing said network policy to said respective edge switch for controlling said user.

6. (New) A method as in claim 5 wherein said providing step (h) comprises providing policy information in said request packet and at said respective edge switch extracting said policy information from said reply packet.

7. (New) A method as in claim 5 wherein said providing step (h) comprises delivering policy information to said respective edge switch subsequent to said returning step (g).

8. (New) A method as in claim 5 wherein said control message snooping conforms to Internet Control Message Protocol (ICMP).

9. (New) A method of enforcing a network policy on a user connected by way of a respective edge switch to a packet – based communication network which has a network core and a plurality of edge switches, the method comprising:

(a) enabling control message snooping for each of said edge switches;

(b) obtaining the network address of said user;

(c) forwarding to said user from a policy server a unicast request packet which has the network address of said user as a destination address, includes a control message protocol header that identifies said unicast packet as a request packet and includes a payload;

(d) in response to reception of said request packet at said user, returning a reply packet which includes said payload unmodified and includes a modifier flag which indicates that said payload is unmodified;

(e) at said respective edge switch, snooping said reply packet and diverting said reply packet to a management agent for said respective edge switch;

(f) parsing said reply packet to determine whether it has an unmodified payload;

(g) modifying said payload;

(h) returning to the policy server said reply packet including said payload as modified, an identification of said respective edge switch and said user; and

(i) providing said network policy to said respective edge switch for controlling said user.

10. (New) A method as in claim 9 wherein said providing step (i) comprises providing policy information in said payload and at said respective edge switch extracting said policy information from said reply packet.

11. (New) A method as in claim 9 wherein said providing step (i) comprises delivering policy information to said respective edge switch subsequent to said returning step (h).

12. (New) A method as in claim 9 wherein said control message snooping conforms to Internet Control Message Protocol (ICMP).

13. (New) A method of enforcing a network policy on a user connected by way of a respective edge switch to a packet – based communication network which has a network core and a plurality of edge switches, the method comprising:

(a) enabling control message snooping for each of said edge switches;

(b) obtaining the network address of said user;

(c) forwarding to said user from a policy server a unicast request packet which has the network address of said user as a destination address, includes a control

(c) forwarding to said user from a policy server a unicast request packet which has the network address of said user as a destination address, includes a control message protocol header that identifies said unicast packet as a request packet and includes a payload including policy information intended for the enforcement of network policy on said user;

(d) in response to reception of said request packet at said user, returning a reply packet which includes said payload unmodified;

(e) at said respective edge switch, snooping said repoly packet and diverting said reply packet to a management agent for said respective edge switch;

(f) parsing said reply packet to determine whether it has an unmodified payload;

(g) extracting said policy information from said payload for use by said switch in respect of said user;

(h) modifying said payload; and

(i) returning to the policy server said reply packet including said payload as modified.

14. (New) A method as in claim 13 wherein said payload as modified includes an identification of said user and an identification of said respective edge switch.

15. (New) A method as in claim 13 wherein said reply packet includes a modifier flag to denote whether said payload is modified or unmodified.

16. (New) A method as in claim 15 wherein said control message snooping conforms to Internet Control Message protocol (ICMP).